Amendments to the Claims:

This listing of claims will replace all prior version, and listings, of claims in the application.

Listing of Claims:

1 (Previously Presented) A method for controlling access to file on a server over a network, the method comprising:

(a) allowing a content originator to publish a file on a first server and to specify what users are authorized to access to file;

(b) replicating the file from the first server on a second server;

(c) in response to receiving a URL request from a client for a file from the first server, determining if a user of the client has been granted authorization to access the file, wherein a client address apparent to the first server differs from a client address apparent to the second server;

(d) generating a transfer ticket from the first server to the client that includes an identifier identifying the particular file on the second server if the user has been granted authorization access, wherein the transfer ticket is not bound to the client address apparent to the first server;

(e) in response to receiving the transfer ticket from the client by the second server, redirecting the client back to the second server with a URL ticket, wherein the URL ticket is bound to the client address apparent to the second server; and

(f) in response to receiving the URL ticket from the client, verifying the URL ticket on the second server and returning the file .

2 (Canceled)

3 (Original) The method of claim 1 wherein step (c) further includes the step of: using a web browser for the client, wherein the web browser has not been customized to request tickets.

4 (Original) The method of claim 1 wherein step (a) further includes the step of: allowing the content originator to specify what access privileges each user has with respect to the files, the access privileges including read, write, and delete.

5 (Original) The method of claim 4 wherein step (a) further includes the step of: allowing the access controls to be specified before and after the file is replicated onto the second server.

6 (Original) The method of claim 4 wherein step (a) further includes the steps of: storing the name of the file in a database along with access privileges specified for the file, and when a user makes a request to access the file, looking up the name of the file in the database and determining if the user has been granted access to the file.

7 (Canceled).

8 (Previously Presented) The method of claim 1 wherein step (e) further includes the step of: placing into the URL ticket a path parameter, a start parameter, a use-by parameter, an end parameter, a uid parameter, a clientid parameter, a sessionid

parameter, a referrer parameter, and a message authentication code (MAC).

9 (Previously Presented) The method of claim 8 wherein step (e) further includes the step of: binding a combination of “basedir+path+sessionid” to an IP address of the client at first use of the URL ticket.

10 (Previously Presented) The method of claim 9 wherein step (e) further includes the step of: verifying the URL ticket as valid when;

(i) the MAC is correct,

(ii) a current time is between values of the start and use-by parameters, or the "basedir+path+sessionID" combination has previously been used for the same IP address,

(iii) the "basedir+path+sessionID" combination has not been used from a different IP address, and

(iv) the URL requests a file that is in a subtree rooted by basedir+"/"path.

11 (Canceled)

12 (Original) The method of claim 1 further including the step of providing a content server as the first server and providing at least one replica server as the second server.

13 (Previously Presented) A system for controlling access to file on a server over a network, the system comprising:

means for allowing a content originator to publish a file on a first server and to specify what users are authorized to access to the file, wherein files on the first server are replicated on a second server;

means responsive to receiving a URL request from a client for a file from the first server for determining if a user of the client has been granted authorization to access the file, wherein a client address apparent to the first server differs from a client address apparent to the second server;

means for generating a transfer ticket from the first server to the client that includes an identifier identifying the particular file on the second server if the user has been granted authorization access, wherein the transfer ticket is not bound to the client address apparent to the first server;

means for receiving the transfer ticket from the client by the second server and redirecting the client back to the second server with a URL ticket, wherein the URL ticket is bound to the client address apparent to the second server; and

means for verifying the URL ticket on the second server and returning the file.

14 (Canceled)

15 (Original) The system of claim 13 wherein the client comprises a web browser that has not been customized to request tickets.

16 (Original) The system of claim 13 wherein the content originator specifies what access privileges each user has with respect to the files, the access privileges including read, write, and delete.

17 (Original) The system of claim 16 wherein the access controls can be specified before and after the file is replicated onto the second server.

18 (Original) The system of claim 16 wherein a name of the file is stored in a database along with the access privileges specified for the file, and when a user makes a request to access the file, the name of the file is looked up in the database to determine if the user has been granted access to the file.

19 (Canceled).

20 (Previously Presented) The system of claim 13 wherein the URL ticket includes a path parameter, a start parameter, a use-by parameter, an end parameter, a uid parameter, a clientid parameter, a sessionid parameter, a referrer parameter, and a message authentication code (MAC).

21 (Original) The system of claim 20 wherein a combination of "basedir+path+sessionid" is bound to an IP address of the client at first use of the URL ticket.

22 (Original) The system of claim 21 wherein the URL ticket is verified as valid when;

(i) the MAC is correct,

(ii) a current time is between values of the start and use-by parameters, or the "basedir+path+sessionID" combination has previously been used for the same IP address,

(iii) the "basedir+path+sessionID" combination has not been used from a different IP address, and

(iv) the URL requests a file that is in a subtree rooted by basedir+"/"path.

23 (Canceled)

24 (Original) The system of claim 13 wherein the first server comprises a content server and the second server comprises at least one replica server.

25 (Previously Presented) A computer-readable medium containing program instructions for controlling access to file on a server over a network, the program instructions for:

(a) allowing a content originator to publish a file on a first server and to specify what users are authorized to access to file;

(b) replicating the file from the first server on a second server;

(c) in response to receiving a URL request from a client for a file from the first server, determining if a user of the client has been granted authorization to access the file, wherein a client address apparent to the first server differs from a client address apparent to the second server;

(d) generating a transfer ticket that includes an identifier identifying the particular file on the second server if the user has been granted authorization access, wherein the transfer ticket is not bound to the client address apparent to the first server;

(e) in response to receiving the transfer ticket from the client by the second server, redirecting the client back to the second server with a URL ticket, wherein the URL ticket is bound to the client address apparent to the second server; and

(f) in response to receiving the URL ticket from the client, verifying the URl ticket on the second server and returning the file.

26 (Canceled)

27 (Previously Presented) The computer-readable medium of claim 25 wherein instruction (c) further includes the instruction of: using a web browser for the client, wherein the web browser has not been customized to request tickets.

28 (Previously Presented) The computer-readable medium of claim 25 wherein instruction (a) further includes the instruction of: allowing the content originator to specify what access privileges each user has with respect to the files, the access privileges including read, write, and delete.

29 (Previously Presented) The computer-readable medium of claim 28 wherein instruction (a) further includes the instruction of: allowing the access controls to be specified before and after the file is replicated onto the second server.

30 (Previously Presented) The computer-readable medium of claim 28 wherein instruction (a) further includes the instructions of: storing the name of the file in a

database along with access privileges specified for the file, and when a user makes a request to access the file, looking up the name of the file in the database and determining if the user has been granted access to the file.

31 (Canceled).

32 (Previously Presented) The computer-readable medium of claim 25 wherein instruction (e) further includes the instruction of: placing into the URL ticket a path parameter, a start parameter, a use-by parameter, an end parameter, a uid parameter, a clientid parameter, a sessionid parameter, a referrer parameter, and a message authentication code (MAC).

33 (Previously Presented) The computer-readable medium of claim 25 wherein instruction (e) further includes the instruction of: binding a combination of "basedir+path+sessionid" to an IP address of the client at first use of the URL ticket.

34 (Previously Presented) The computer-readable medium of claim 33 wherein instruction (g) further includes the instruction of: verifying the URL ticket as valid when;

(i) the MAC is correct,

(ii) a current time is between values of the start and use-by parameters, or the "basedir+path+sessionID" combination has previously been used for the same IP address,

(iii) the "basedir+path+sessionID" combination has not been used from a different IP address, and

(iv) the URL requests a file that is in a subtree rooted by basedir+"/"path.

35 (Canceled)

36 (Previously Presented) The computer-readable medium of claim 25 further including the instruction of providing a content server as the first server and providing at least one replica server as the second server.

37 (Canceled)

38 (Canceled)